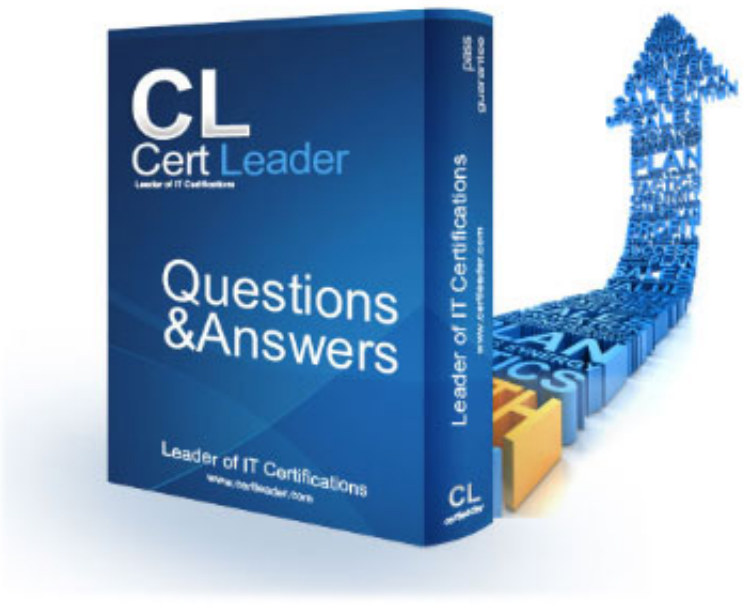
CISSP Dumps

Certified Information Systems Security Professional (CISSP)

https://www.certleader.com/CISSP-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
A company whose Information Technology (IT) services are being delivered from a Tier 4 data center, is preparing a companywide Business Continuity Planning (BCP). Which of the following failures should the IT manager be concerned with?

A. Application
B. Storage
C. Power
D. Network

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

A. Only when assets are clearly defined
B. Only when standards are defined
C. Only when controls are put in place
D. Only procedures are defined

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

A. Install mantraps at the building entrances
B. Enclose the personnel entry area with polycarbonate plastic
C. Supply a duress alarm for personnel exposed to the public
D. Hire a guard to protect the public area

Answer: D

NEW QUESTION 4
- (Exam Topic 3)
The use of private and public encryption keys is fundamental in the implementation of which of the following?

A. Diffie-Hellman algorithm
B. Secure Sockets Layer (SSL)
C. Advanced Encryption Standard (AES)
D. Message Digest 5 (MD5)

Answer: A

NEW QUESTION 5
- (Exam Topic 4)
Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

A. Packet filtering
B. Port services filtering
C. Content filtering
D. Application access control

Answer: A

NEW QUESTION 6
- (Exam Topic 4)
An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

A. Implement packet filtering on the network firewalls
B. Install Host Based Intrusion Detection Systems (HIDS)
C. Require strong authentication for administrators
D. Implement logical network segmentation at the switches

Answer: D

NEW QUESTION 7
- (Exam Topic 4)
What is the purpose of an Internet Protocol (IP) spoofing attack?

A. To send excessive amounts of data to a process, making it unpredictable
B. To intercept network traffic without authorization

C. To disguise the destination address from a target's IP filtering devices
D. To convince a system that it is communicating with a known entity

Answer: D

NEW QUESTION 8
- (Exam Topic 5)
Users require access rights that allow them to view the average salary of groups of employees. Which control would prevent the users from obtaining an individual employee's salary?

A. Limit access to predefined queries
B. Segregate the database into a small number of partitions each with a separate security level
C. Implement Role Based Access Control (RBAC)
D. Reduce the number of people who have access to the system for statistical purposes

Answer: C

NEW QUESTION 9
- (Exam Topic 7)
A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

A. Guaranteed recovery of all business functions
B. Minimization of the need decision making during a crisis
C. Insurance against litigation following a disaster
D. Protection from loss of organization resources

Answer: D

NEW QUESTION 10
- (Exam Topic 7)
A continuous information security monitoring program can BEST reduce risk through which of the following?

A. Collecting security events and correlating them to identify anomalies
B. Facilitating system-wide visibility into the activities of critical user accounts
C. Encompassing people, process, and technology
D. Logging both scheduled and unscheduled system changes

Answer: B

NEW QUESTION 10
- (Exam Topic 7)
An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

A. Absence of a Business Intelligence (BI) solution
B. Inadequate cost modeling
C. Improper deployment of the Service-Oriented Architecture (SOA)
D. Insufficient Service Level Agreement (SLA)

Answer: D

NEW QUESTION 13
- (Exam Topic 7)
What is the PRIMARY reason for implementing change management?

A. Certify and approve releases to the environment
B. Provide version rollbacks for system changes
C. Ensure that all applications are approved
D. Ensure accountability for changes to the environment

Answer: D

NEW QUESTION 17
- (Exam Topic 7)
When is a Business Continuity Plan (BCP) considered to be valid?

A. When it has been validated by the Business Continuity (BC) manager
B. When it has been validated by the board of directors
C. When it has been validated by all threat scenarios
D. When it has been validated by realistic exercises

Answer: D

NEW QUESTION 22
- (Exam Topic 7)

Which of the following is the FIRST step in the incident response process?

A. Determine the cause of the incident
B. Disconnect the system involved from the network
C. Isolate and contain the system involved
D. Investigate all symptoms to confirm the incident

Answer: D

NEW QUESTION 24
- (Exam Topic 9)
Which of the following is a method used to prevent Structured Query Language (SQL) injection attacks?

A. Data compression
B. Data classification
C. Data warehousing
D. Data validation

Answer: D

NEW QUESTION 29
- (Exam Topic 9)
Which one of the following is a threat related to the use of web-based client side input validation?

A. Users would be able to alter the input after validation has occurred
B. The web server would not be able to validate the input after transmission
C. The client system could receive invalid input from the web server
D. The web server would not be able to receive invalid input from the client

Answer: A

NEW QUESTION 30
- (Exam Topic 9)
A vulnerability test on an Information System (IS) is conducted to

A. exploit security weaknesses in the IS.
B. measure system performance on systems with weak security controls.
C. evaluate the effectiveness of security controls.
D. prepare for Disaster Recovery (DR) planning.

Answer: C

NEW QUESTION 33
- (Exam Topic 9)
An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?

A. Data leakage
B. Unfiltered channel
C. Data emanation
D. Covert channel

Answer: D

NEW QUESTION 37
- (Exam Topic 9)
In the area of disaster planning and recovery, what strategy entails the presentation of information about the plan?

A. Communication
B. Planning
C. Recovery
D. Escalation

Answer: A

NEW QUESTION 39
- (Exam Topic 9)
The key benefits of a signed and encrypted e-mail include

A. confidentiality, authentication, and authorization.
B. confidentiality, non-repudiation, and authentication.
C. non-repudiation, authorization, and authentication.
D. non-repudiation, confidentiality, and authorization.

Answer: B

NEW QUESTION 44
- (Exam Topic 9)
What technique BEST describes antivirus software that detects viruses by watching anomalous behavior?

A. Signature
B. Inference
C. Induction
D. Heuristic

Answer: D

NEW QUESTION 49
- (Exam Topic 9)
Which one of the following transmission media is MOST effective in preventing data interception?

A. Microwave
B. Twisted-pair
C. Fiber optic
D. Coaxial cable

Answer: C

NEW QUESTION 53
- (Exam Topic 9)
Which layer of the Open Systems Interconnections (OSI) model implementation adds information concerning the logical connection between the sender and receiver?

A. Physical
B. Session
C. Transport
D. Data-Link

Answer: C

NEW QUESTION 56
- (Exam Topic 9)
What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

A. Man-in-the-Middle (MITM) attack
B. Smurfing
C. Session redirect
D. Spoofing

Answer: D

NEW QUESTION 57
- (Exam Topic 9)
The overall goal of a penetration test is to determine a system's

A. ability to withstand an attack.
B. capacity management.
C. error recovery capabilities.
D. reliability under stress.

Answer: A

NEW QUESTION 62
- (Exam Topic 9)
Multi-threaded applications are more at risk than single-threaded applications to

A. race conditions.
B. virus infection.
C. packet sniffing.
D. database injection.

Answer: A

NEW QUESTION 66
- (Exam Topic 9)
Which of the following is an attacker MOST likely to target to gain privileged access to a system?

A. Programs that write to system resources
B. Programs that write to user directories
C. Log files containing sensitive information
D. Log files containing system calls

Answer:

A

NEW QUESTION 68
- (Exam Topic 9)
Which of the following is an authentication protocol in which a new random number is generated uniquely for each login session?

A. Challenge Handshake Authentication Protocol (CHAP)
B. Point-to-Point Protocol (PPP)
C. Extensible Authentication Protocol (EAP)
D. Password Authentication Protocol (PAP)

Answer: A

NEW QUESTION 69
- (Exam Topic 9)
How can a forensic specialist exclude from examination a large percentage of operating system files residing on a copy of the target system?

A. Take another backup of the media in question then delete all irrelevant operating system files.
B. Create a comparison database of cryptographic hashes of the files from a system with the same operating system and patch level.
C. Generate a message digest (MD) or secure hash on the drive image to detect tampering of the media being examined.
D. Discard harmless files for the operating system, and known installed programs.

Answer: B

NEW QUESTION 74
- (Exam Topic 9)
Which of the following is the best practice for testing a Business Continuity Plan (BCP)?

A. Test before the IT Audit
B. Test when environment changes
C. Test after installation of security patches
D. Test after implementation of system patches

Answer: B

NEW QUESTION 77
- (Exam Topic 9)
A security professional has just completed their organization's Business Impact Analysis (BIA). Following Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) best practices, what would be the professional's NEXT step?

A. Identify and select recovery strategies.
B. Present the findings to management for funding.
C. Select members for the organization's recovery teams.
D. Prepare a plan to test the organization's ability to recover its operations.

Answer: A

NEW QUESTION 80
- (Exam Topic 9)
As one component of a physical security system, an Electronic Access Control (EAC) token is BEST known for its ability to

A. overcome the problems of key assignments.
B. monitor the opening of windows and doors.
C. trigger alarms when intruders are detected.
D. lock down a facility during an emergency.

Answer: A

NEW QUESTION 82
- (Exam Topic 9)
What security management control is MOST often broken by collusion?

A. Job rotation
B. Separation of duties
C. Least privilege model
D. Increased monitoring

Answer: B

NEW QUESTION 86
- (Exam Topic 9)
Which of the following is an essential element of a privileged identity lifecycle management?

A. Regularly perform account re-validation and approval
B. Account provisioning based on multi-factor authentication
C. Frequently review performed activities and request justification

D. Account information to be provided by supervisor or line manager

Answer: A

NEW QUESTION 87
- (Exam Topic 9)
Which one of the following security mechanisms provides the BEST way to restrict the execution of privileged procedures?

A. Role Based Access Control (RBAC)
B. Biometric access control
C. Federated Identity Management (IdM)
D. Application hardening

Answer: A

NEW QUESTION 88
- (Exam Topic 9)
Which one of the following describes granularity?

A. Maximum number of entries available in an Access Control List (ACL)
B. Fineness to which a trusted system can authenticate users
C. Number of violations divided by the number of total accesses
D. Fineness to which an access control system can be adjusted

Answer: D

NEW QUESTION 91
- (Exam Topic 9)
Which of the following is the MOST important consideration when storing and processing Personally Identifiable Information (PII)?

A. Encrypt and hash all PII to avoid disclosure and tampering.
B. Store PII for no more than one year.
C. Avoid storing PII in a Cloud Service Provider.
D. Adherence to collection limitation laws and regulations.

Answer: D

NEW QUESTION 96
- (Exam Topic 9)
What would be the PRIMARY concern when designing and coordinating a security assessment for an Automatic Teller Machine (ATM) system?

A. Physical access to the electronic hardware
B. Regularly scheduled maintenance process
C. Availability of the network connection
D. Processing delays

Answer: A

NEW QUESTION 97
- (Exam Topic 9)
An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the MOST effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

A. Implement packet filtering on the network firewalls
B. Require strong authentication for administrators
C. Install Host Based Intrusion Detection Systems (HIDS)
D. Implement logical network segmentation at the switches

Answer: D

NEW QUESTION 101
- (Exam Topic 9)
Which of the following is a security limitation of File Transfer Protocol (FTP)?

A. Passive FTP is not compatible with web browsers.
B. Anonymous access is allowed.
C. FTP uses Transmission Control Protocol (TCP) ports 20 and 21.
D. Authentication is not encrypted.

Answer: D

NEW QUESTION 105
- (Exam Topic 9)
A security consultant has been asked to research an organization's legal obligations to protect privacy-related information. What kind of reading material is MOST relevant to this project?

A. The organization's current security policies concerning privacy issues
B. Privacy-related regulations enforced by governing bodies applicable to the organization
C. Privacy best practices published by recognized security standards organizations
D. Organizational procedures designed to protect privacy information

Answer: B

NEW QUESTION 108
- (Exam Topic 9)
Which of the following is the FIRST step of a penetration test plan?

A. Analyzing a network diagram of the target network
B. Notifying the company's customers
C. Obtaining the approval of the company's management
D. Scheduling the penetration test during a period of least impact

Answer: C

NEW QUESTION 112
- (Exam Topic 9)
What is an effective practice when returning electronic storage media to third parties for repair?

A. Ensuring the media is not labeled in any way that indicates the organization's name.
B. Disassembling the media and removing parts that may contain sensitive datA.
C. Physically breaking parts of the media that may contain sensitive datA.
D. Establishing a contract with the third party regarding the secure handling of the mediA.

Answer: D

NEW QUESTION 114
- (Exam Topic 9)
Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy contain?

A. An Explanation: of how long the data subject's collected information will be retained for and how it will be eventually disposed.
B. An Explanation: of who can be contacted at the organization collecting the information if corrections are required by the data subject.
C. An Explanation: of the regulatory frameworks and compliance standards the information collecting organization adheres to.
D. An Explanation: of all the technologies employed by the collecting organization in gathering information on the data subject.

Answer: B

NEW QUESTION 116
- (Exam Topic 9)
When implementing controls in a heterogeneous end-point network for an organization, it is critical that

A. hosts are able to establish network communications.
B. users can make modifications to their security software configurations.
C. common software security components be implemented across all hosts.
D. firewalls running on each host are fully customizable by the user.

Answer: C

NEW QUESTION 119
- (Exam Topic 9)
Which of the following defines the key exchange for Internet Protocol Security (IPSec)?

A. Secure Sockets Layer (SSL) key exchange
B. Internet Key Exchange (IKE)
C. Security Key Exchange (SKE)
D. Internet Control Message Protocol (ICMP)

Answer: B

NEW QUESTION 123
- (Exam Topic 9)
Why MUST a Kerberos server be well protected from unauthorized access?

A. It contains the keys of all clients.
B. It always operates at root privilege.
C. It contains all the tickets for services.
D. It contains the Internet Protocol (IP) address of all network entities.

Answer: A

NEW QUESTION 127
- (Exam Topic 9)

A software scanner identifies a region within a binary image having high entropy. What does this MOST likely indicate?

A. Encryption routines
B. Random number generator
C. Obfuscated code
D. Botnet command and control

Answer: C

NEW QUESTION 128
- (Exam Topic 9)
Which of the following is a potential risk when a program runs in privileged mode?

A. It may serve to create unnecessary code complexity
B. It may not enforce job separation duties
C. It may create unnecessary application hardening
D. It may allow malicious code to be inserted

Answer: D

NEW QUESTION 132
- (Exam Topic 9)
By allowing storage communications to run on top of Transmission Control Protocol/Internet Protocol (TCP/IP) with a Storage Area Network (SAN), the

A. confidentiality of the traffic is protected.
B. opportunity to sniff network traffic exists.
C. opportunity for device identity spoofing is eliminated.
D. storage devices are protected against availability attacks.

Answer: B

NEW QUESTION 137
- (Exam Topic 9)
Which of the following BEST represents the principle of open design?

A. Disassembly, analysis, or reverse engineering will reveal the security functionality of the computer system.
B. Algorithms must be protected to ensure the security and interoperability of the designed system.
C. A knowledgeable user should have limited privileges on the system to prevent their ability to compromise security capabilities.
D. The security of a mechanism should not depend on the secrecy of its design or implementation.

Answer: D

NEW QUESTION 141
- (Exam Topic 9)
An engineer in a software company has created a virus creation tool. The tool can generate thousands of polymorphic viruses. The engineer is planning to use the tool in a controlled environment to test the company's next generation virus scanning software. Which would BEST describe the behavior of the engineer and why?

A. The behavior is ethical because the tool will be used to create a better virus scanner.
B. The behavior is ethical because any experienced programmer could create such a tool.
C. The behavior is not ethical because creating any kind of virus is bad.
D. The behavior is not ethical because such a tool could be leaked on the Internet.

Answer: A

NEW QUESTION 144
- (Exam Topic 9)
At a MINIMUM, a formal review of any Disaster Recovery Plan (DRP) should be conducted

A. monthly.
B. quarterly.
C. annually.
D. bi-annually.

Answer: C

NEW QUESTION 146
- (Exam Topic 9)
In Disaster Recovery (DR) and business continuity training, which BEST describes a functional drill?

A. A full-scale simulation of an emergency and the subsequent response functions
B. A specific test by response teams of individual emergency response functions
C. A functional evacuation of personnel
D. An activation of the backup site

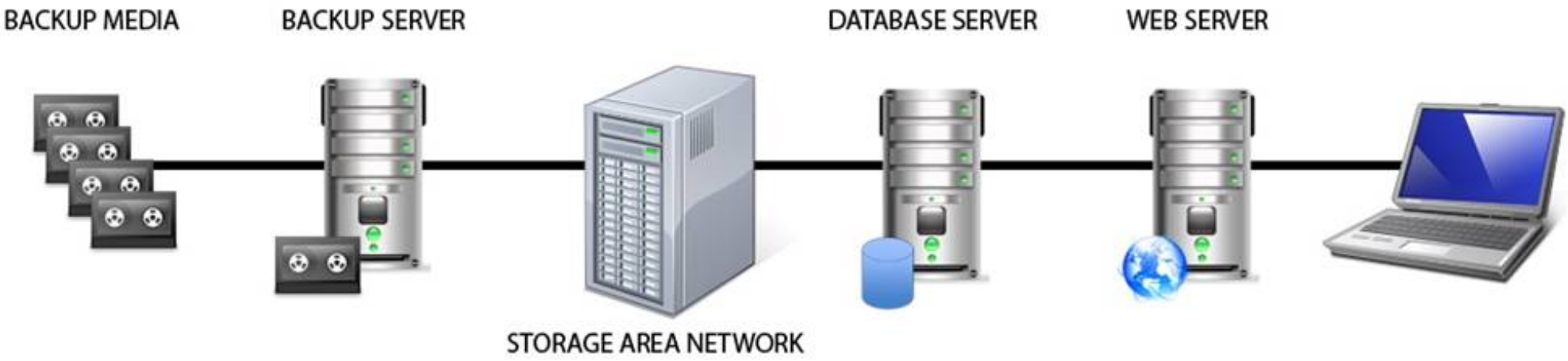
Answer: B

NEW QUESTION 151
- (Exam Topic 10)
Refer to the information below to answer the question.
A new employee is given a laptop computer with full administrator access. This employee does not have a personal computer at home and has a child that uses the computer to send and receive e-mail, search the web, and use instant messaging. The organization's Information Technology (IT) department discovers that a peer-to-peer program has been installed on the computer using the employee's access.
Which of the following solutions would have MOST likely detected the use of peer-to-peer programs when the computer was connected to the office network?

A. Anti-virus software
B. Intrusion Prevention System (IPS)
C. Anti-spyware software
D. Integrity checking software

Answer: B

NEW QUESTION 156
- (Exam Topic 10)
Identify the component that MOST likely lacks digital accountability related to information access. Click on the correct device in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Backup Media
Reference: Official (ISC)2 Guide to the CISSP CBK, Third Edition page 1029

NEW QUESTION 159
- (Exam Topic 10)
Which of the following is the BEST reason to review audit logs periodically?

A. Verify they are operating properly
B. Monitor employee productivity
C. Identify anomalies in use patterns
D. Meet compliance regulations

Answer: C

NEW QUESTION 161
- (Exam Topic 10)
According to best practice, which of the following groups is the MOST effective in performing an information security compliance audit?

A. In-house security administrators
B. In-house Network Team
C. Disaster Recovery (DR) Team
D. External consultants

Answer: D

NEW QUESTION 163
- (Exam Topic 10)
Refer to the information below to answer the question.
A security practitioner detects client-based attacks on the organization's network. A plan will be necessary to address these concerns.
In addition to web browsers, what PRIMARY areas need to be addressed concerning mobile code used for malicious purposes?

A. Text editors, database, and Internet phone applications
B. Email, presentation, and database applications
C. Image libraries, presentation and spreadsheet applications
D. Email, media players, and instant messaging applications

Answer: D

NEW QUESTION 164
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.
What MUST the access control logs contain in addition to the identifier?

A. Time of the access
B. Security classification
C. Denied access attempts
D. Associated clearance

Answer: A

NEW QUESTION 166
- (Exam Topic 10)
What is the MOST critical factor to achieve the goals of a security program?

A. Capabilities of security resources
B. Executive management support
C. Effectiveness of security management
D. Budget approved for security resources

Answer: B

NEW QUESTION 171
- (Exam Topic 10)
What is the PRIMARY advantage of using automated application security testing tools?

A. The application can be protected in the production environment.
B. Large amounts of code can be tested using fewer resources.
C. The application will fail less when tested using these tools.
D. Detailed testing of code functions can be performed.

Answer: B

NEW QUESTION 175
- (Exam Topic 10)
A security manager has noticed an inconsistent application of server security controls resulting in vulnerabilities on critical systems. What is the MOST likely cause of this issue?

A. A lack of baseline standards
B. Improper documentation of security guidelines
C. A poorly designed security policy communication program
D. Host-based Intrusion Prevention System (HIPS) policies are ineffective

Answer: A

NEW QUESTION 180
- (Exam Topic 10)
Refer to the information below to answer the question.
During the investigation of a security incident, it is determined that an unauthorized individual accessed a system which hosts a database containing financial information.
If the intrusion causes the system processes to hang, which of the following has been affected?

A. System integrity
B. System availability
C. System confidentiality
D. System auditability

Answer: B

NEW QUESTION 185
- (Exam Topic 10)
Which of the following methods provides the MOST protection for user credentials?

A. Forms-based authentication
B. Digest authentication
C. Basic authentication
D. Self-registration

Answer: B

NEW QUESTION 187
- (Exam Topic 10)
Refer to the information below to answer the question.
In a Multilevel Security (MLS) system, the following sensitivity labels are used in increasing levels of sensitivity: restricted, confidential, secret, top secret. Table A lists the clearance levels for four users, while Table B lists the security classes of four different files.

Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

In a Bell-LaPadula system, which user cannot write to File 3?

A. User A
B. User B
C. User C
D. User D

Answer: D

NEW QUESTION 192
- (Exam Topic 10)
Which of the following is a BEST practice when traveling internationally with laptops containing Personally Identifiable Information (PII)?

A. Use a thumb drive to transfer information from a foreign computer.
B. Do not take unnecessary information, including sensitive information.
C. Connect the laptop only to well-known networks like the hotel or public Internet cafes.
D. Request international points of contact help scan the laptop on arrival to ensure it is protected.

Answer: B

NEW QUESTION 194
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization has hired an information security officer to lead their security department. The officer has adequate people resources but is lacking the other necessary components to have an effective security program. There are numerous initiatives requiring security involvement.
Which of the following is considered the MOST important priority for the information security officer?

A. Formal acceptance of the security strategy
B. Disciplinary actions taken against unethical behavior
C. Development of an awareness program for new employees
D. Audit of all organization system configurations for faults

Answer: A

NEW QUESTION 198
- (Exam Topic 10)
A large bank deploys hardware tokens to all customers that use their online banking system. The token generates and displays a six digit numeric password every 60 seconds. The customers must log into their bank accounts using this numeric password. This is an example of

A. asynchronous token.
B. Single Sign-On (SSO) token.
C. single factor authentication token.
D. synchronous token.

Answer: D

NEW QUESTION 202
- (Exam Topic 10)
A system is developed so that its business users can perform business functions but not user administration functions. Application administrators can perform administration functions but not user business functions. These capabilities are BEST described as

A. least privilege.
B. rule based access controls.
C. Mandatory Access Control (MAC).
D. separation of duties.

Answer: D

NEW QUESTION 203
- (Exam Topic 10)
Refer to the information below to answer the question.
A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access.

The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes. Following best practice, where should the permitted access for each department and job classification combination be specified?

A. Security procedures
B. Security standards
C. Human resource policy
D. Human resource standards

Answer: B

NEW QUESTION 208
- (Exam Topic 10)
Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

A. Secondary use of the data by business users
B. The organization's security policies and standards
C. The business purpose for which the data is to be used
D. The overall protection of corporate resources and data

Answer: B

NEW QUESTION 213
- (Exam Topic 10)
Host-Based Intrusion Protection (HIPS) systems are often deployed in monitoring or learning mode during their initial implementation. What is the objective of starting in this mode?

A. Automatically create exceptions for specific actions or files
B. Determine which files are unsafe to access and blacklist them
C. Automatically whitelist actions or files known to the system
D. Build a baseline of normal or safe system events for review

Answer: D

NEW QUESTION 214
- (Exam Topic 10)
A Business Continuity Plan (BCP) is based on

A. the policy and procedures manual.
B. an existing BCP from a similar organization.
C. a review of the business processes and procedures.
D. a standard checklist of required items and objectives.

Answer: C

NEW QUESTION 217
- (Exam Topic 10)
The use of proximity card to gain access to a building is an example of what type of security control?

A. Legal
B. Logical
C. Physical
D. Procedural

Answer: C

NEW QUESTION 218
- (Exam Topic 10)
A large university needs to enable student access to university resources from their homes. Which of the following provides the BEST option for low maintenance and ease of deployment?

A. Provide students with Internet Protocol Security (IPSec) Virtual Private Network (VPN) client software.
B. Use Secure Sockets Layer (SSL) VPN technology.
C. Use Secure Shell (SSH) with public/private keys.
D. Require students to purchase home router capable of VPN.

Answer: B

NEW QUESTION 221
- (Exam Topic 10)
The amount of data that will be collected during an audit is PRIMARILY determined by the

A. audit scope.
B. auditor's experience level.
C. availability of the datA.
D. integrity of the datA.

Answer: A

NEW QUESTION 226
- (Exam Topic 10)
Refer to the information below to answer the question.
Desktop computers in an organization were sanitized for re-use in an equivalent security environment. The data was destroyed in accordance with organizational policy and all marking and other external indications of the sensitivity of the data that was formerly stored on the magnetic drives were removed.
After magnetic drives were degaussed twice according to the product manufacturer's directions, what is the MOST LIKELY security issue with degaussing?

A. Commercial products often have serious weaknesses of the magnetic force available in the degausser product.
B. Degausser products may not be properly maintained and operated.
C. The inability to turn the drive around in the chamber for the second pass due to human error.
D. Inadequate record keeping when sanitizing mediA.

Answer: B

NEW QUESTION 227
- (Exam Topic 10)
For a service provider, which of the following MOST effectively addresses confidentiality concerns for customers using cloud computing?

A. Hash functions
B. Data segregation
C. File system permissions
D. Non-repudiation controls

Answer: B

NEW QUESTION 231
- (Exam Topic 10)
Refer to the information below to answer the question.
An organization experiencing a negative financial impact is forced to reduce budgets and the number of Information Technology (IT) operations staff performing basic logical access security administration functions. Security processes have been tightly integrated into normal IT operations and are not separate and distinct roles.
When determining appropriate resource allocation, which of the following is MOST important to monitor?

A. Number of system compromises
B. Number of audit findings
C. Number of staff reductions
D. Number of additional assets

Answer: B

NEW QUESTION 234
- (Exam Topic 10)
Which of the following provides the MOST protection against data theft of sensitive information when a laptop is stolen?

A. Set up a BIOS and operating system password
B. Encrypt the virtual drive where confidential files can be stored
C. Implement a mandatory policy in which sensitive data cannot be stored on laptops, but only on the corporate network
D. Encrypt the entire disk and delete contents after a set number of failed access attempts

Answer: D

NEW QUESTION 237
- (Exam Topic 10)
What is the MOST important reason to configure unique user IDs?

A. Supporting accountability
B. Reducing authentication errors
C. Preventing password compromise
D. Supporting Single Sign On (SSO)

Answer: A

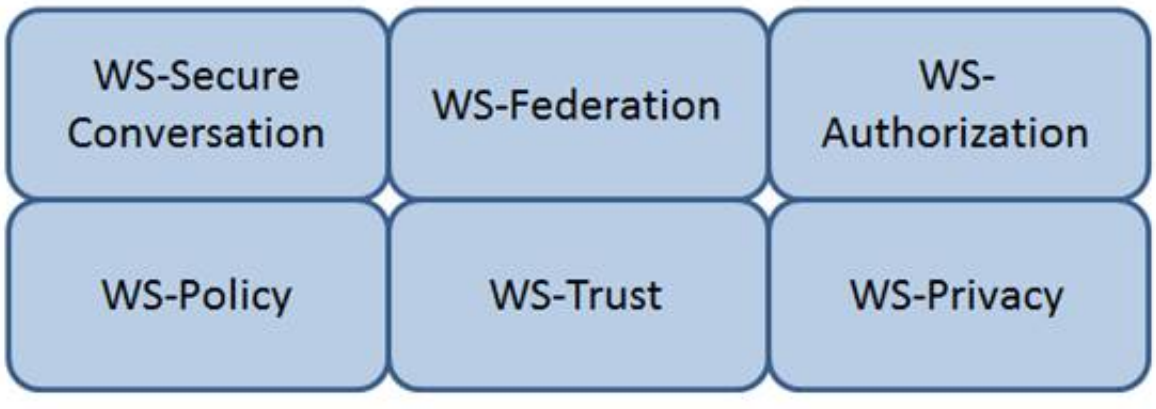
NEW QUESTION 241
- (Exam Topic 11)
What is the process called when impact values are assigned to the security objectives for information types?

A. Qualitative analysis
B. Quantitative analysis
C. Remediation
D. System security categorization

Answer: D

NEW QUESTION 243
- (Exam Topic 11)
Which Web Services Security (WS-Security) specification handles the management of security tokens and the underlying policies for granting access? Click on the

correct specification in the image below.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
WS-Authorization
Reference: Java Web Services: Up and Running" By Martin Kalin page 228

NEW QUESTION 248
- (Exam Topic 11)
Which of the following prevents improper aggregation of privileges in Role Based Access Control (RBAC)?

A. Hierarchical inheritance
B. Dynamic separation of duties
C. The Clark-Wilson security model
D. The Bell-LaPadula security model

Answer: B

NEW QUESTION 251
- (Exam Topic 11)
A security professional has been asked to evaluate the options for the location of a new data center within a multifloor building. Concerns for the data center include emanations and physical access controls.
Which of the following is the BEST location?

A. On the top floor
B. In the basement
C. In the core of the building
D. In an exterior room with windows

Answer: C

NEW QUESTION 254
- (Exam Topic 11)
What is the GREATEST challenge to identifying data leaks?

A. Available technical tools that enable user activity monitoring.
B. Documented asset classification policy and clear labeling of assets.
C. Senior management cooperation in investigating suspicious behavior.
D. Law enforcement participation to apprehend and interrogate suspects.

Answer: B

NEW QUESTION 259
- (Exam Topic 11)
Which of the following statements is TRUE regarding state-based analysis as a functional software testing technique?

A. It is useful for testing communications protocols and graphical user interfaces.
B. It is characterized by the stateless behavior of a process implemented in a function.
C. Test inputs are obtained from the derived boundaries of the given functional specifications.
D. An entire partition can be covered by considering only one representative value from that partition.

Answer: A

NEW QUESTION 262
- (Exam Topic 11)
Data remanence refers to which of the following?

A. The remaining photons left in a fiber optic cable after a secure transmission.
B. The retention period required by law or regulation.
C. The magnetic flux created when removing the network connection from a server or personal computer.
D. The residual information left on magnetic storage media after a deletion or erasure.

Answer: D

NEW QUESTION 265
- (Exam Topic 11)
Which of the following is the MOST important element of change management documentation?

A. List of components involved
B. Number of changes being made
C. Business case justification
D. A stakeholder communication

Answer: C

NEW QUESTION 266
- (Exam Topic 11)
What should happen when an emergency change to a system must be performed?

A. The change must be given priority at the next meeting of the change control board.
B. Testing and approvals must be performed quickly.
C. The change must be performed immediately and then submitted to the change board.
D. The change is performed and a notation is made in the system log.

Answer: B

NEW QUESTION 271
- (Exam Topic 11)
After a thorough analysis, it was discovered that a perpetrator compromised a network by gaining access to the network through a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway. The perpetrator guessed a username and brute forced the password to gain access. Which of the following BEST mitigates this issue?

A. Implement strong passwords authentication for VPN
B. Integrate the VPN with centralized credential stores
C. Implement an Internet Protocol Security (IPSec) client
D. Use two-factor authentication mechanisms

Answer: D

NEW QUESTION 272
- (Exam Topic 11)
Which of the following has the GREATEST impact on an organization's security posture?

A. International and country-specific compliance requirements
B. Security violations by employees and contractors
C. Resource constraints due to increasing costs of supporting security
D. Audit findings related to employee access and permissions process

Answer: A

NEW QUESTION 277
- (Exam Topic 11)
A mobile device application that restricts the storage of user information to just that which is needed to accomplish lawful business goals adheres to what privacy principle?

A. Onward transfer
B. Collection Limitation
C. Collector Accountability
D. Individual Participation

Answer: B

NEW QUESTION 278
- (Exam Topic 11)
Disaster Recovery Plan (DRP) training material should be

A. consistent so that all audiences receive the same training.
B. stored in a fire proof safe to ensure availability when needed.
C. only delivered in paper format.
D. presented in a professional looking manner.

Answer: A

NEW QUESTION 280
- (Exam Topic 11)
Which of the following is most helpful in applying the principle of LEAST privilege?

A. Establishing a sandboxing environment
B. Setting up a Virtual Private Network (VPN) tunnel
C. Monitoring and reviewing privileged sessions
D. Introducing a job rotation program

Answer: A

NEW QUESTION 281
- (Exam Topic 11)
Single Sign-On (SSO) is PRIMARILY designed to address which of the following?

A. Confidentiality and Integrity
B. Availability and Accountability
C. Integrity and Availability
D. Accountability and Assurance

Answer: D

NEW QUESTION 282
- (Exam Topic 11)
Discretionary Access Control (DAC) restricts access according to

A. data classification labeling.
B. page views within an application.
C. authorizations granted to the user.
D. management accreditation.

Answer: C

NEW QUESTION 285
- (Exam Topic 11)
Which of the following are Systems Engineering Life Cycle (SELC) Technical Processes?

A. Concept, Development, Production, Utilization, Support, Retirement
B. Stakeholder Requirements Definition, Architectural Design, Implementation, Verification, Operation
C. Acquisition, Measurement, Configuration Management, Production, Operation, Support
D. Concept, Requirements, Design, Implementation, Production, Maintenance, Support, Disposal

Answer: B

NEW QUESTION 289
- (Exam Topic 11)
What is the PRIMARY difference between security policies and security procedures?

A. Policies are used to enforce violations, and procedures create penalties
B. Policies point to guidelines, and procedures are more contractual in nature
C. Policies are included in awareness training, and procedures give guidance
D. Policies are generic in nature, and procedures contain operational details

Answer: D

NEW QUESTION 292
- (Exam Topic 11)
Which of the following explains why record destruction requirements are included in a data retention policy?

A. To comply with legal and business requirements
B. To save cost for storage and backup
C. To meet destruction guidelines
D. To validate data ownership

Answer: A

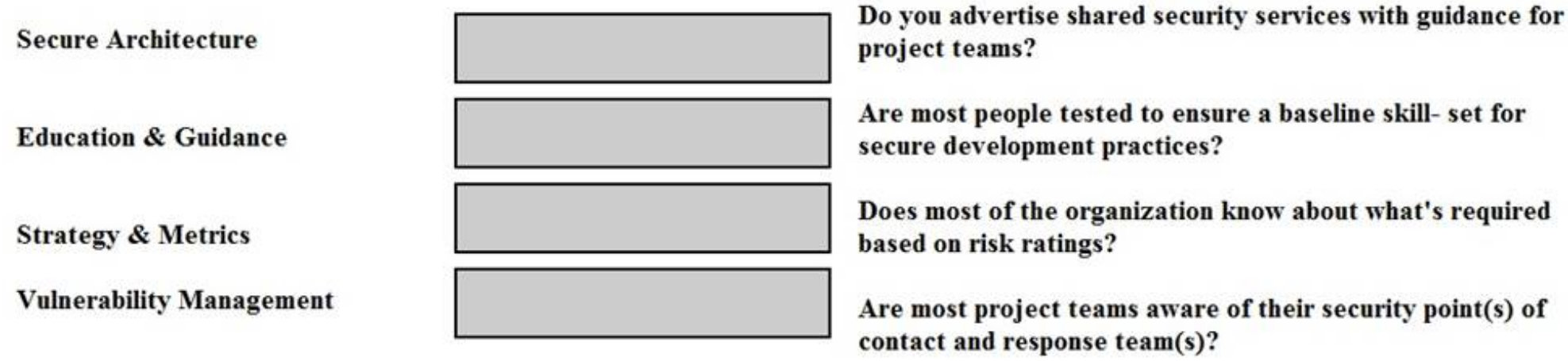
NEW QUESTION 295
- (Exam Topic 11)

Which of the following is the PRIMARY concern when using an Internet browser to access a cloud-based service?

A. Insecure implementation of Application Programming Interfaces (API)
B. Improper use and storage of management keys
C. Misconfiguration of infrastructure allowing for unauthorized access
D. Vulnerabilities within protocols that can expose confidential data

Answer: D

NEW QUESTION 297
- (Exam Topic 11)
Match the objectives to the assessment questions in the governance domain of Software Assurance Maturity Model (SAMM).



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 302
- (Exam Topic 11)
A security professional is asked to provide a solution that restricts a bank teller to only perform a savings deposit transaction but allows a supervisor to perform corrections after the transaction. Which of the following is the MOST effective solution?

A. Access is based on rules.
B. Access is determined by the system.
C. Access is based on user's role.
D. Access is based on data sensitivity.

Answer: C

NEW QUESTION 306
- (Exam Topic 11)
Secure Sockets Layer (SSL) encryption protects

A. data at rest.
B. the source IP address.
C. data transmitted.
D. data availability.

Answer: C

NEW QUESTION 311
- (Exam Topic 11)
The implementation of which features of an identity management system reduces costs and administration overhead while improving audit and accountability?

A. Two-factor authentication

B. Single Sign-On (SSO)
C. User self-service
D. A metadirectory

Answer: C

NEW QUESTION 315
- (Exam Topic 11)
Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering		Definition
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Threat Assessment		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Protection Needs		The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Risk		The method used to identify feasible security **risk mitigation options and plans.**

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Security Engineering		Definition
Security Risk Treatment	Protection Needs	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Threat Assessment	Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Protection Needs	Threat Assessment	The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Risk	Security Risk Treatment	The method used to identify feasible security **risk mitigation options and plans.**

NEW QUESTION 317
- (Exam Topic 11)
Sensitive customer data is going to be added to a database. What is the MOST effective implementation for ensuring data privacy?

A. Discretionary Access Control (DAC) procedures
B. Mandatory Access Control (MAC) procedures
C. Data link encryption
D. Segregation of duties

Answer: B

NEW QUESTION 320
- (Exam Topic 11)
Software Code signing is used as a method of verifying what security concept?

A. Integrity
B. Confidentiality
C. Availability
D. Access Control

Answer: A

NEW QUESTION 322

- (Exam Topic 11)
What does an organization FIRST review to assure compliance with privacy requirements?

A. Best practices
B. Business objectives
C. Legal and regulatory mandates
D. Employee's compliance to policies and standards

Answer: C

NEW QUESTION 325
- (Exam Topic 11)
The goal of a Business Continuity Plan (BCP) training and awareness program is to

A. enhance the skills required to create, maintain, and execute the plan.
B. provide for a high level of recovery in case of disaster.
C. describe the recovery organization to new employees.
D. provide each recovery team with checklists and procedures.

Answer: A

NEW QUESTION 329
- (Exam Topic 11)
Which one of the following operates at the session, transport, or network layer of the Open System Interconnection (OSI) model?

A. Data at rest encryption
B. Configuration Management
C. Integrity checking software
D. Cyclic redundancy check (CRC)

Answer: D

NEW QUESTION 330
- (Exam Topic 11)
What type of test assesses a Disaster Recovery (DR) plan using realistic disaster scenarios while maintaining minimal impact to business operations?

A. Parallel
B. Walkthrough
C. Simulation
D. Tabletop

Answer: C

NEW QUESTION 334
- (Exam Topic 11)
Which of the following questions can be answered using user and group entitlement reporting?

A. When a particular file was last accessed by a user
B. Change control activities for a particular group of users
C. The number of failed login attempts for a particular user
D. Where does a particular user have access within the network

Answer: D

NEW QUESTION 338
- (Exam Topic 11)
For an organization considering two-factor authentication for secure network access, which of the following is MOST secure?

A. Challenge response and private key
B. Digital certificates and Single Sign-On (SSO)
C. Tokens and passphrase
D. Smart card and biometrics

Answer: D

NEW QUESTION 340
- (Exam Topic 11)
Which of the following is a recommended alternative to an integrated email encryption system?

A. Sign emails containing sensitive data
B. Send sensitive data in separate emails
C. Encrypt sensitive data separately in attachments
D. Store sensitive information to be sent in encrypted drives

Answer: C

NEW QUESTION 344
- (Exam Topic 11)
Which of the following activities BEST identifies operational problems, security misconfigurations, and malicious attacks?

A. Policy documentation review
B. Authentication validation
C. Periodic log reviews
D. Interface testing

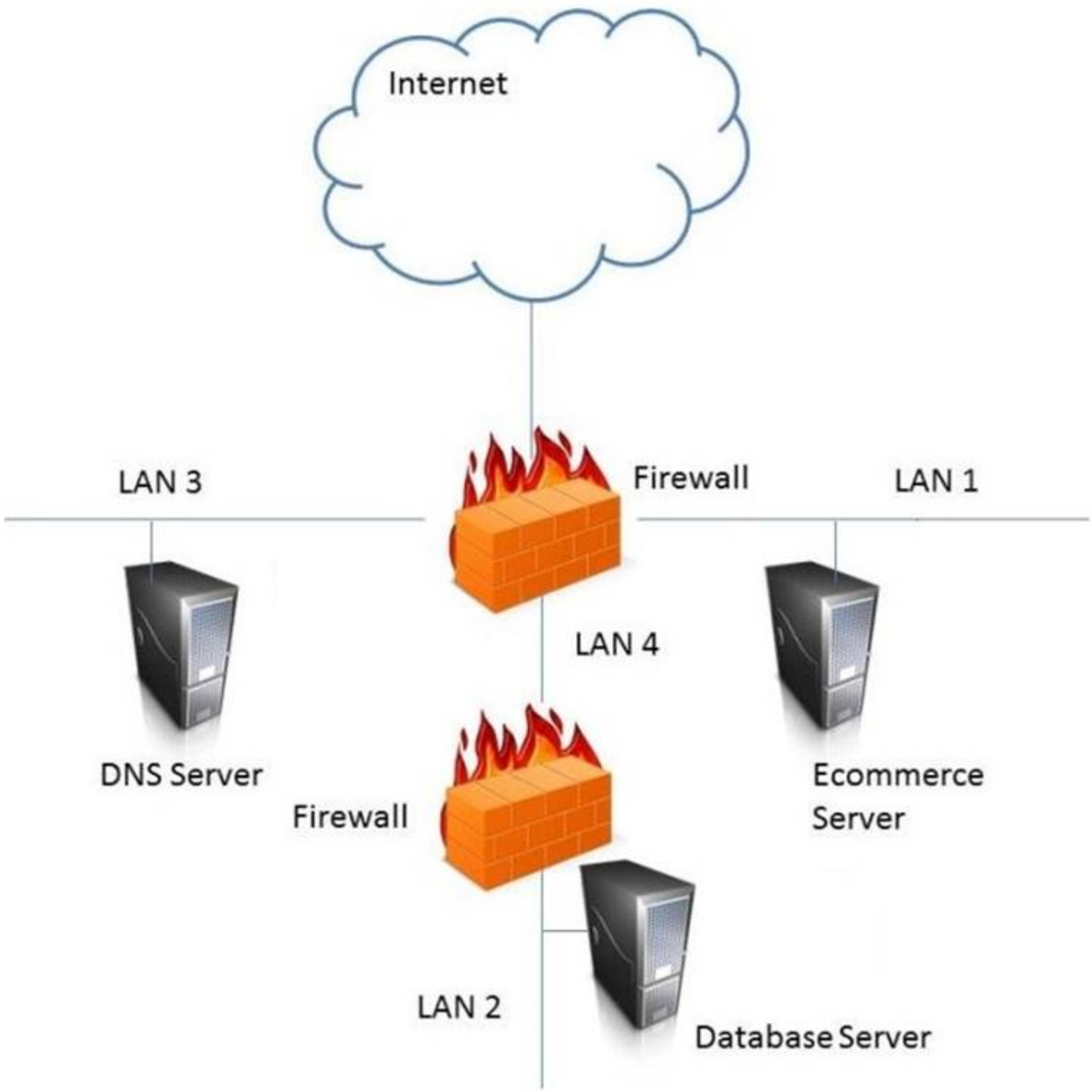
Answer: C

NEW QUESTION 348
- (Exam Topic 11)
The 802.1x standard provides a framework for what?

A. Network authentication for only wireless networks
B. Network authentication for wired and wireless networks
C. Wireless encryption using the Advanced Encryption Standard (AES)
D. Wireless network encryption using Secure Sockets Layer (SSL)

Answer: B

NEW QUESTION 350
- (Exam Topic 11)
In the network design below, where is the MOST secure Local Area Network (LAN) segment to deploy a Wireless Access Point (WAP) that provides contractors access to the Internet and authorized enterprise services?



A. Mastered
B. Not Mastered

Answer: A

Explanation:
LAN 4

NEW QUESTION 352
- (Exam Topic 11)
Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

A. Application interface entry and endpoints
B. The likelihood and impact of a vulnerability
C. Countermeasures and mitigations for vulnerabilities
D. A data flow diagram for the application and attack surface analysis

Answer: D

NEW QUESTION 353
- (Exam Topic 11)
In order for a security policy to be effective within an organization, it MUST include

A. strong statements that clearly define the problem.
B. a list of all standards that apply to the policy.
C. owner information and date of last revision.
D. disciplinary measures for non compliance.

Answer: D

NEW QUESTION 357
- (Exam Topic 11)
The BEST method to mitigate the risk of a dictionary attack on a system is to

A. use a hardware token.
B. use complex passphrases.
C. implement password history.
D. encrypt the access control list (ACL).

Answer: A

NEW QUESTION 360
- (Exam Topic 11)
The MAIN reason an organization conducts a security authorization process is to

A. force the organization to make conscious risk decisions.
B. assure the effectiveness of security controls.
C. assure the correct security organization exists.
D. force the organization to enlist management support.

Answer: A

NEW QUESTION 365
- (Exam Topic 12)
What is the difference between media marking and media labeling?

A. Media marking refers to the use of human-readable security attributes, while media labeling refers to the use of security attributes in internal data structures.
B. Media labeling refers to the use of human-readable security attributes, while media marking refers to the use of security attributes in internal data structures.
C. Media labeling refers to security attributes required by public policy/law, while media marking refers to security required by internal organizational policy.
D. Media marking refers to security attributes required by public policy/law, while media labeling refers to security attributes required by internal organizational policy.

Answer: D

NEW QUESTION 370
- (Exam Topic 12)
Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

A. Addresses and protocols of network-based logs are analyzed.
B. Host-based system logging has files stored in multiple locations.
C. Properly handled network-based logs may be more reliable and valid.
D. Network-based systems cannot capture users logging into the console.

Answer: A

NEW QUESTION 371
- (Exam Topic 12)
The PRIMARY outcome of a certification process is that it provides documented

A. interconnected systems and their implemented security controls.
B. standards for security assessment, testing, and process evaluation.
C. system weakness for remediation.
D. security analyses needed to make a risk-based decision.

Answer: D

NEW QUESTION 375
- (Exam Topic 12)
Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

A. Job rotation
B. Separation of duties
C. Least privilege
D. Mandatory vacations

Answer: B

NEW QUESTION 377
- (Exam Topic 12)
An application developer is deciding on the amount of idle session time that the application allows before a timeout. The BEST reason for determining the session timeout requirement is

A. organization policy.
B. industry best practices.
C. industry laws and regulations.
D. management feedback.

Answer: A

NEW QUESTION 381
- (Exam Topic 12)
What type of wireless network attack BEST describes an Electromagnetic Pulse (EMP) attack?

A. Radio Frequency (RF) attack
B. Denial of Service (DoS) attack
C. Data modification attack
D. Application-layer attack

Answer: B

NEW QUESTION 385
- (Exam Topic 12)
Which of the following is an advantage of on-premise Credential Management Systems?

A. Lower infrastructure capital costs
B. Control over system configuration
C. Reduced administrative overhead
D. Improved credential interoperability

Answer: B

NEW QUESTION 387
- (Exam Topic 12)
Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

A. dig
B. ipconfig
C. ifconfig
D. nbstat

Answer: A

NEW QUESTION 390
- (Exam Topic 12)
Determining outage costs caused by a disaster can BEST be measured by the

A. cost of redundant systems and backups.
B. cost to recover from an outage.
C. overall long-term impact of the outage.
D. revenue lost during the outage.

Answer: C

NEW QUESTION 391

- (Exam Topic 12)
How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

A. Examines log messages or other indications on the system.
B. Monitors alarms sent to the system administrator
C. Matches traffic patterns to virus signature files
D. Examines the Access Control List (ACL)

Answer: C

NEW QUESTION 393
- (Exam Topic 12)
Which of the following BEST represents the concept of least privilege?

A. Access to an object is denied unless access is specifically allowed.
B. Access to an object is only available to the owner.
C. Access to an object is allowed unless it is protected by the information security policy.
D. Access to an object is only allowed to authenticated users via an Access Control List (ACL).

Answer: A

NEW QUESTION 394
- (Exam Topic 12)
Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

A. VPN bandwidth
B. Simultaneous connection to other networks
C. Users with Internet Protocol (IP) addressing conflicts
D. Remote users with administrative rights

Answer: B

NEW QUESTION 396
- (Exam Topic 12)
Which of the following is the PRIMARY reason for employing physical security personnel at entry points in facilities where card access is in operation?

A. To verify that only employees have access to the facility.
B. To identify present hazards requiring remediation.
C. To monitor staff movement throughout the facility.
D. To provide a safe environment for employees.

Answer: D

NEW QUESTION 400
- (Exam Topic 12)
Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

A. Length of Initialization Vector (IV)
B. Protection against message replay
C. Detection of message tampering
D. Built-in provision to rotate keys

Answer: A

NEW QUESTION 405
- (Exam Topic 12)
Which of the following are effective countermeasures against passive network-layer attacks?

A. Federated security and authenticated access controls
B. Trusted software development and run time integrity controls
C. Encryption and security enabled applications
D. Enclave boundary protection and computing environment defense

Answer: C

NEW QUESTION 410
- (Exam Topic 12)
What is the MOST important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

A. Management support
B. Consideration of organizational need
C. Technology used for delivery
D. Target audience

Answer: B

NEW QUESTION 413
- (Exam Topic 12)
When building a data classification scheme, which of the following is the PRIMARY concern?

A. Purpose
B. Cost effectiveness
C. Availability
D. Authenticity

Answer: D

NEW QUESTION 414
- (Exam Topic 12)
Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

A. Notification tool
B. Message queuing tool
C. Security token tool
D. Synchronization tool

Answer: C

NEW QUESTION 418
- (Exam Topic 12)
What balance MUST be considered when web application developers determine how informative application error messages should be constructed?

A. Risk versus benefit
B. Availability versus auditability
C. Confidentiality versus integrity
D. Performance versus user satisfaction

Answer: A

NEW QUESTION 422
- (Exam Topic 12)
What is a characteristic of Secure Socket Layer (SSL) and Transport Layer Security (TLS)?

A. SSL and TLS provide a generic channel security mechanism on top of Transmission Control Protocol (TCP).
B. SSL and TLS provide nonrepudiation by default.
C. SSL and TLS do not provide security for most routed protocols.
D. SSL and TLS provide header encapsulation over HyperText Transfer Protocol (HTTP).

Answer: A

NEW QUESTION 424
- (Exam Topic 13)
Which of the following is the BEST reason for writing an information security policy?

A. To support information security governance
B. To reduce the number of audit findings
C. To deter attackers
D. To implement effective information security controls

Answer: A

NEW QUESTION 425
- (Exam Topic 13)
Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

A. Implement processes for automated removal of access for terminated employees.
B. Delete employee network and system IDs upon termination.
C. Manually remove terminated employee user-access to all systems and applications.
D. Disable terminated employee network ID to remove all access.

Answer: B

NEW QUESTION 427
- (Exam Topic 13)
A control to protect from a Denial-of-Service (DoS) attach has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

A. 25%
B. 50%
C. 75%
D. 100%

Answer:

A

NEW QUESTION 432
- (Exam Topic 13)
What is the MAIN goal of information security awareness and training?

A. To inform users of the latest malware threats
B. To inform users of information assurance responsibilities
C. To comply with the organization information security policy
D. To prepare students for certification

Answer: B

NEW QUESTION 436
- (Exam Topic 13)
In an organization where Network Access Control (NAC) has been deployed, a device trying to connect to the network is being placed into an isolated domain. What could be done on this device in order to obtain proper connectivity?

A. Connect the device to another network jack
B. Apply remediation's according to security requirements
C. Apply Operating System (OS) patches
D. Change the Message Authentication Code (MAC) address of the network interface

Answer: B

NEW QUESTION 439
- (Exam Topic 13)
As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

A. Use a web scanner to scan for vulnerabilities within the website.
B. Perform a code review to ensure that the database references are properly addressed.
C. Establish a secure connection to the web server to validate that only the approved ports are open.
D. Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

Answer: D

NEW QUESTION 443
- (Exam Topic 13)
An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?

A. Aggregate it into one database in the US
B. Process it in the US, but store the information in France
C. Share it with a third party
D. Anonymize it and process it in the US

Answer: C

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 444
- (Exam Topic 13)
What is the PRIMARY role of a scrum master in agile development?

A. To choose the primary development language
B. To choose the integrated development environment
C. To match the software requirements to the delivery plan
D. To project manage the software delivery

Answer: D

NEW QUESTION 446
- (Exam Topic 13)
Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

A. Truncating parts of the data
B. Applying Access Control Lists (ACL) to the data
C. Appending non-watermarked data to watermarked data
D. Storing the data in a database

Answer: A

NEW QUESTION 450

- (Exam Topic 13)
Drag the following Security Engineering terms on the left to the BEST definition on the right.

Security Engineering Term		Definition
Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment		The method used to identify feasible security risk mitigation options and plans.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.
Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

NEW QUESTION 454
- (Exam Topic 13)
Which of the following combinations would MOST negatively affect availability?

A. Denial of Service (DoS) attacks and outdated hardware
B. Unauthorized transactions and outdated hardware
C. Fire and accidental changes to data
D. Unauthorized transactions and denial of service attacks

Answer: A

NEW QUESTION 459
- (Exam Topic 13)
The design review for an application has been completed and is ready for release. What technique should an organization use to assure application integrity?

A. Application authentication
B. Input validation
C. Digital signing
D. Device encryption

Answer: C

NEW QUESTION 462
- (Exam Topic 13)
Which security modes is MOST commonly used in a commercial environment because it protects the integrity of financial and accounting data?

A. Biba
B. Graham-Denning
C. Clark-Wilson
D. Beil-LaPadula

Answer: C

NEW QUESTION 465
- (Exam Topic 13)
Which of the following is a characteristic of an internal audit?

A. An internal audit is typically shorter in duration than an external audit.
B. The internal audit schedule is published to the organization well in advance.
C. The internal auditor reports to the Information Technology (IT) department
D. Management is responsible for reading and acting upon the internal audit results

Answer: D

NEW QUESTION 469
- (Exam Topic 13)
What is the MAIN purpose of a change management policy?

A. To assure management that changes to the Information Technology (IT) infrastructure are necessary
B. To identify the changes that may be made to the Information Technology (IT) infrastructure
C. To verify that changes to the Information Technology (IT) infrastructure are approved
D. To determine the necessary for implementing modifications to the Information Technology (IT) infrastructure

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 472
- (Exam Topic 13)
What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

A. The IDS can detect failed administrator logon attempts from servers.
B. The IDS can increase the number of packets to analyze.
C. The firewall can increase the number of packets to analyze.
D. The firewall can detect failed administrator login attempts from servers

Answer: A

NEW QUESTION 475
- (Exam Topic 13)
The organization would like to deploy an authorization mechanism for an Information Technology (IT) infrastructure project with high employee turnover.
Which access control mechanism would be preferred?

A. Attribute Based Access Control (ABAC)
B. Discretionary Access Control (DAC)
C. Mandatory Access Control (MAC)
D. Role-Based Access Control (RBAC)

Answer: D

NEW QUESTION 478
- (Exam Topic 13)
Which of the following is a common characteristic of privacy?

A. Provision for maintaining an audit trail of access to the private data
B. Notice to the subject of the existence of a database containing relevant credit card data
C. Process for the subject to inspect and correct personal data on-site
D. Database requirements for integration of privacy data

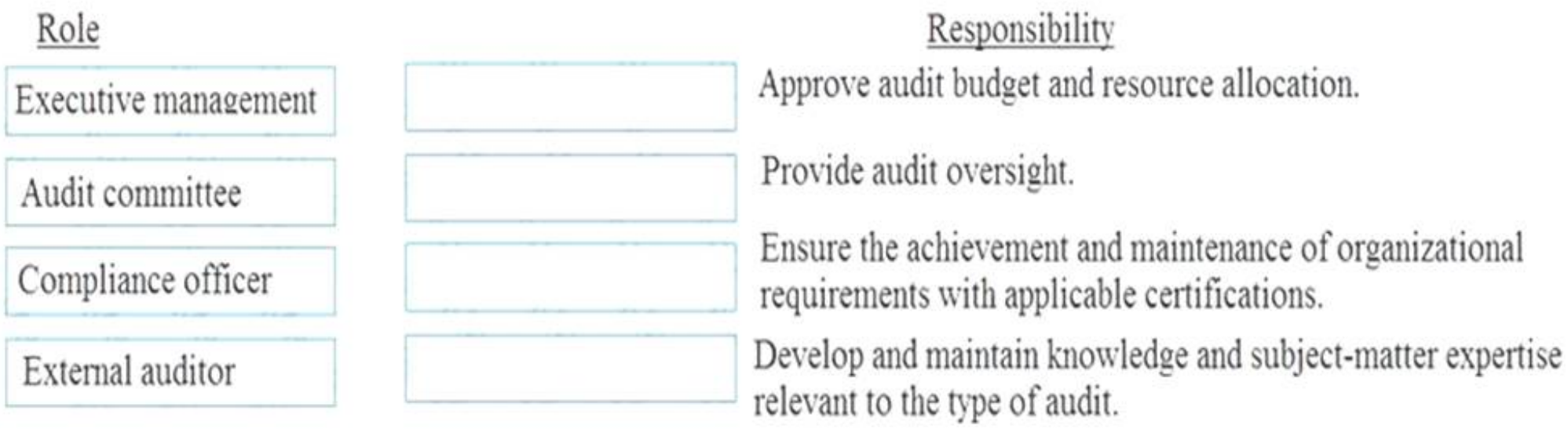
Answer: A

NEW QUESTION 483
- (Exam Topic 13)
Which type of test would an organization perform in order to locate and target exploitable defects?

A. Penetration
B. System
C. Performance
D. Vulnerability

Answer: A

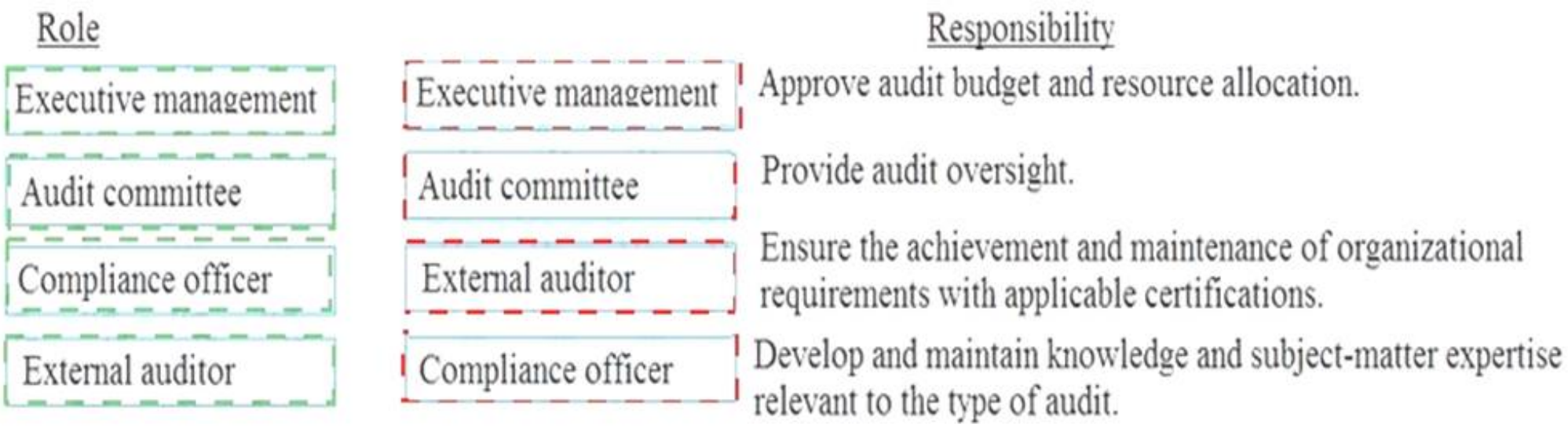
NEW QUESTION 488
- (Exam Topic 13)
Match the functional roles in an external audit to their responsibilities. Drag each role on the left to its corresponding responsibility on the right. Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 492
- (Exam Topic 13)
Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

A. Security governance
B. Risk management
C. Security portfolio management
D. Risk assessment

Answer: B

NEW QUESTION 493
- (Exam Topic 13)
Which of the following would MINIMIZE the ability of an attacker to exploit a buffer overflow?

A. Memory review
B. Code review
C. Message division
D. Buffer division

Answer: B

NEW QUESTION 498
- (Exam Topic 13)
When developing a business case for updating a security program, the security program owner MUST do which of the following?

A. Identify relevant metrics
B. Prepare performance test reports
C. Obtain resources for the security program
D. Interview executive management

Answer: A

NEW QUESTION 500
- (Exam Topic 13)
Which of the following mandates the amount and complexity of security controls applied to a security risk?

A. Security vulnerabilities
B. Risk tolerance
C. Risk mitigation
D. Security staff

Answer: C

NEW QUESTION 503
- (Exam Topic 13)
Who is accountable for the information within an Information System (IS)?

A. Security manager
B. System owner
C. Data owner
D. Data processor

Answer: B

Explanation:
Section: Security Operations

NEW QUESTION 507
- (Exam Topic 13)
A chemical plan wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade.
Which of the following is the GREATEST impact on security for the network?

A. The network administrators have no knowledge of ICS
B. The ICS is now accessible from the office network
C. The ICS does not support the office password policy
D. RS422 is more reliable than Ethernet

Answer: B

NEW QUESTION 511
- (Exam Topic 13)
Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

A. Erase
B. Sanitize
C. Encrypt
D. Degauss

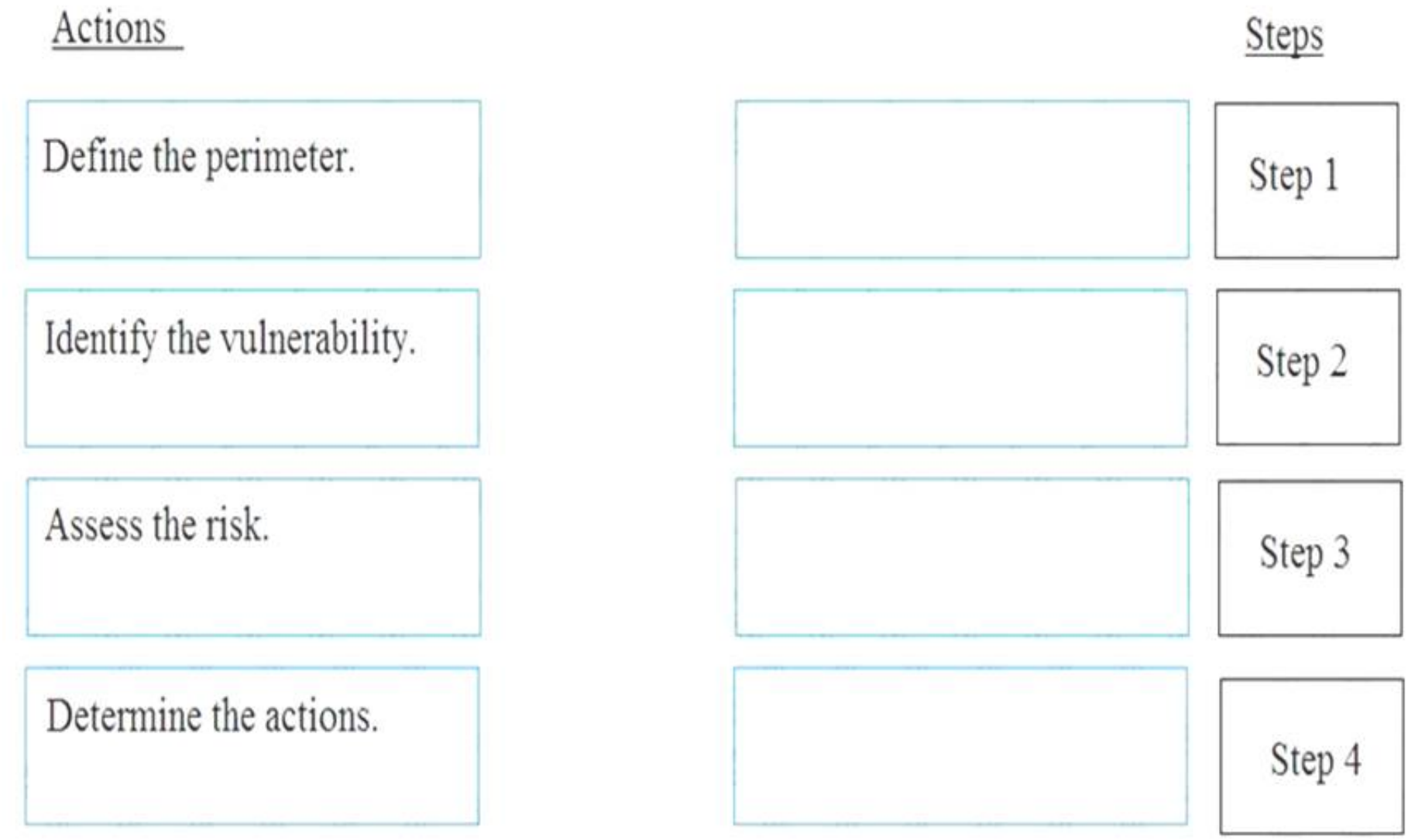
Answer: B

NEW QUESTION 512
- (Exam Topic 13)
A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device. Which of the following is MOST effective to mitigate future infections?

A. Develop a written organizational policy prohibiting unauthorized USB devices
B. Train users on the dangers of transferring data in USB devices
C. Implement centralized technical control of USB port connections
D. Encrypt removable USB devices containing data at rest

Answer: C

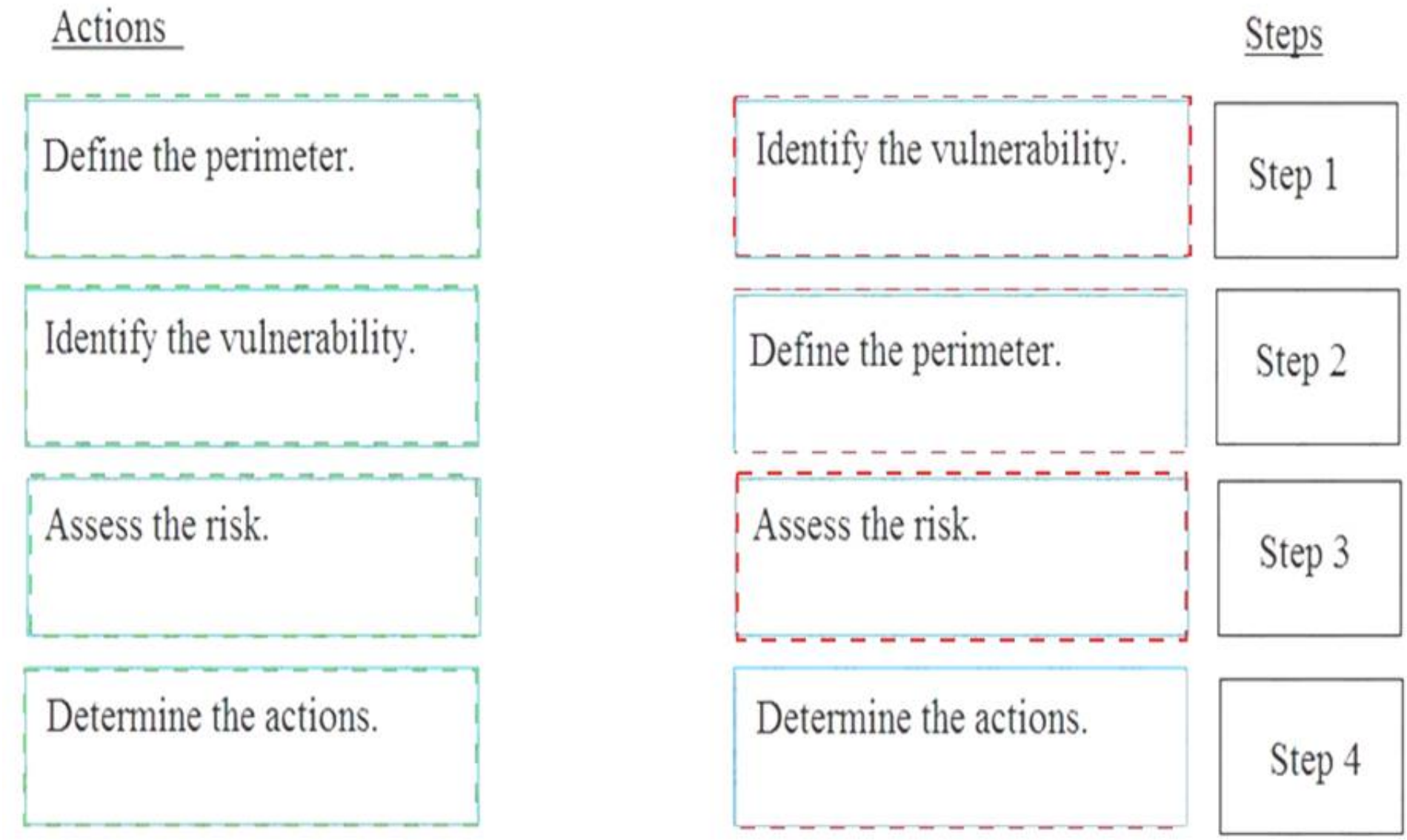
NEW QUESTION 515
- (Exam Topic 13)
What is the correct order of steps in an information security assessment?
Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 516
- (Exam Topic 13)
During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):

http://www.companysite.com/products/products.asp?productid=123
or 1=1
What type of attack does this indicate?

A. Directory traversal
B. Structured Query Language (SQL) injection
C. Cross-Site Scripting (XSS)
D. Shellcode injection

Answer: C

NEW QUESTION 519
- (Exam Topic 13)
Attack trees are MOST useful for which of the following?

A. Determining system security scopes
B. Generating attack libraries
C. Enumerating threats
D. Evaluating Denial of Service (DoS) attacks

Answer: A

NEW QUESTION 523
- (Exam Topic 13)
A Security Operations Center (SOC) receives an incident response notification on a server with an active intruder who has planted a backdoor. Initial notifications are sent and communications are established. What MUST be considered or evaluated before performing the next step?

A. Notifying law enforcement is crucial before hashing the contents of the server hard drive
B. Identifying who executed the incident is more important than how the incident happened
C. Removing the server from the network may prevent catching the intruder
D. Copying the contents of the hard drive to another storage device may damage the evidence

Answer: C

Explanation:
Section: Security Operations

NEW QUESTION 526
- (Exam Topic 13)
Which of the following is the BEST metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

A. Application connection successes resulting in data leakage
B. Administrative costs for restoring systems after connection failure
C. Employee system timeouts from implementing wrong limits
D. Help desk costs required to support password reset requests

Answer: D

NEW QUESTION 528
- (Exam Topic 13)
Which of the following would BEST support effective testing of patch compatibility when patches are applied to an organization's systems?

A. Standardized configurations for devices
B. Standardized patch testing equipment
C. Automated system patching
D. Management support for patching

Answer: A

Explanation:
Section: Security Assessment and Testing

NEW QUESTION 532
- (Exam Topic 13)
Which of the following is a common feature of an Identity as a Service (IDaaS) solution?

A. Single Sign-On (SSO) authentication support
B. Privileged user authentication support
C. Password reset service support
D. Terminal Access Controller Access Control System (TACACS) authentication support

Answer: A

NEW QUESTION 536

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISSP Exam with Our Prep Materials Via below:

https://www.certleader.com/CISSP-dumps.html